State of California

SECRETARY OF STATE

WITHDRAWAL OF APPROVAL OF HART INTERCIVIC SYSTEM 6.2.1 DRE & OPTICAL SCAN VOTING SYSTEM AND CONDITIONAL RE-APPROVAL OF USE OF HART INTERCIVIC SYSTEM 6.2.1 DRE & OPTICAL SCAN VOTING SYSTEM

Whereas, pursuant to Elections Code section 19201, no voting system, in whole or in part, may be used unless it has received the approval of the Secretary of State; and

Whereas, Elections Code section 19222 requires that I, as Secretary of State for the State of California, conduct periodic reviews of voting systems to determine if they are defective, obsolete, or otherwise unacceptable; and

Whereas, at my inauguration as Secretary of State on January 8, 2007, I announced my intention to conduct a top-to-bottom review of voting systems approved for use in California; and

Whereas, on March 22, 2007, I circulated for public comment draft criteria for a review of voting systems approved for use in California, covering system security issues, access for voters with disabilities, access for minority language voters, and usability for elections officials and poll workers; and

Whereas, pursuant to my statutory obligations, I have undertaken such a review of voting systems approved for use in California, including the Hart Intercivic System 6.2.1 voting system, pursuant to a contract with the Regents of the University of California and conducted by experts selected and supervised by principal investigators from the computer science faculties of the Berkeley and Davis campuses, to determine if the voting systems are defective, obsolete, or otherwise unacceptable for use in the February 5, 2008, Presidential Primary Election and subsequent elections in California; and

Whereas, the study was completed on July 20, 2007, following which the expert reviewers delivered their written reports on their findings and methodology; and

Whereas, the expert reviewers found that the quality of the 2002 Voting System Standards (VSS) to which each of the three systems in their study were certified is inadequate, and noted

further that questions have been raised about the effectiveness of the testing; for example, Ciber, Inc., a testing laboratory involved in testing of voting systems under the 2002 VSS, has been denied interim accreditation for testing voting systems by the Federal Election Assistance Commission after finding that Ciber "was not following its quality-control procedures and could not document that it was conducting all the required tests"; and

Whereas, the expert reviewers demonstrated that the physical and technological security mechanisms provided by the vendors for each of the voting systems analyzed were inadequate to ensure accuracy and integrity of the election results and of the systems that provide those results; and

Whereas, the expert reviewers reported that all of the voting systems studied contain serious design flaws that have led directly to specific vulnerabilities, which attackers could exploit to affect election outcomes; and

Whereas, the Hart Source Code Review Team found that the Hart voting system contains design features that can be used in a fashion for which those design features were not intended, including network interfaces that are not secured against direct attack; and

Whereas, the Hart Source Code Review Team found that the Hart voting system's software fails to check the correctness of inputs from other Hart voting system components and uses those inputs in unsafe ways, potentially enabling an attacker to use voting system components to reprogram voting system units throughout the county with malicious code that would affect a subsequent election; and

Whereas, the Hart Source Code Review Team found that the Hart voting system exhibits a notable lack of the use of cryptographic security protocols to secure network communications, and where cryptography is used, a single countywide symmetric key is used that could allow a person to forge ballot information and election results in multiple polling locations; and

Whereas, the Hart Source Code Review Team found that the Hart voting system allows raw ballot records and other information to be used to reconstruct how each voter voted, potentially compromising the secrecy of the ballot; and

Whereas, the Hart Source Code Review Team found that many attacks are hard to detect and correct, defying development and implementation of simple, effective countermeasures; and

Whereas, the Hart Red Team that conducted penetration testing of the Hart voting system discovered multiple vulnerabilities; and

Whereas, on non-polling place components of the voting system that run on a Windows platform, Hart Red Team members located an undisclosed database user name and password and also manually bypassed Hart software security settings so they could run the Hart software in a standard Windows desktop environment, a possible vector for unauthorized access to the voting system's databases; and

Whereas, Hart Red Team members determined that the Hart voting system software fails to check the correctness of inputs from other Hart voting system components; and

Whereas, Hart Red Team members were able to access device-level menus on the Hart eScan precinct-based optical scan unit that should have been locked with passwords, which could allow access for altering voting system configuration settings; and

Whereas, Hart Red Team members confirmed findings from previous studies that allowed malicious actions to be performed on the Hart eScan precinct-based optical scan unit, including altering vote totals, using tools commonly found in an office; and

Whereas, Hart Red Team members were able to demonstrate the ability, after the close of the polls, to use a laptop computer to tamper with a Mobile Ballot Box memory device used to record votes cast on the eSlate direct decoding electronic voting device, an attack that, if undetected during the tampering, could alter vote totals in a manner not detected by technological safeguards but detectable in a manual recount; and

Whereas, Hart Red Team members found that the Hart voting system allows for remote eavesdropping and capture of the audio narration of a ballot (a feature designed for use by voters with disabilities), potentially violating the secrecy of the ballot; and

Whereas, architectural features of the Hart voting system significantly reduce its vulnerability to a viral attack introduced while the polls are open by a person with access only to the eSlate Direct Recording Electronic voting device; and

Whereas, architectural features of the Hart voting system significantly reduce its vulnerability to viral corruption of the voting system's central tally component through the introduction of malicious code at a polling place; and

Whereas, on July 30, 2007, a duly noticed public hearing was held to give interested persons an opportunity to express their views regarding the review of various voting systems, including the Hart Intercivic System 6.2.1 voting system; at this hearing, approximately 60 individuals testified; many more submitted comments by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, I, as Secretary of State, am authorized to withdraw approval previously granted of any voting system or part of a voting system if I determine that voting system or any part of that voting system to be defective or otherwise unacceptable; and

Whereas, I have reviewed the Hart Intercivic System 6.2.1 voting system and I have reviewed and considered several reports regarding the use of this voting system; the public testimony presented at the duly noticed public hearing held on July 30, 2007; and the comments submitted by letter, facsimile transmission, and electronic mail; and

Whereas, pursuant to Elections Code section 19222, six months' notice must be given before withdrawing approval previously granted of any voting system or part of a voting system unless I, as Secretary of State, for good cause shown, make a determination that a shorter period is necessary; and

Whereas, pursuant to Elections Code section 19222, any withdrawal by the Secretary of State of the previous approval of a voting system or part of a voting system is not effective as to any election conducted within six months of that withdrawal; now

***Therefore*, I, Debra Bowen, Secretary of State for the State of California, find and determine, pursuant to Division 19 of the Elections Code, as follows:**

For the reasons set forth above, the Hart InterCivic System 6.2.1 voting system, comprised of JBC, version 4.3.1, eSlate/DAU, version 4.2.13, eScan, version 1.3.14, VBO, version 1.8.3, eCM Manager, version 1.1.7, Ballot Now software, version 3.3.11, BOSS software, version 4.3.13, Rally software, version 2.3.7, Tally software, version 4.3.10, and SERVO, version 4.2.10, which was previously approved, is found and determined to be defective or unacceptable and its certification and approval for use in subsequent elections in California is immediately withdrawn, except as specifically provided below.

1. Before any use in the February 5, 2008, Presidential primary election, jurisdictions must reinstall all software and firmware (including reformatting all hard disk drives and reinstalling the operating system where applicable) on all election management system servers and workstations, voting devices and hardware components of the voting system. Voting system application software must be reinstalled using the currently approved version obtained directly from the federal testing laboratory or the Secretary of State.

2. Within 30 days of the date of this document, the vendor must present a plan and uniform jurisdiction-use procedures to the Secretary of State for approval that will prevent future viral propagation of malicious software from one system component to another, such as from a voting system component located in one precinct to voting system components located in other precincts. The plan and use procedures must incorporate, or employ methods at least as effective as, a configuration of parallel central election management systems separated by an "air-gap" where (1) a permanent central system known to be running unaltered, certified software and firmware is used solely to define elections and program voting equipment and memory cards, (2) a physically-isolated duplicate system, reformatted after every election to guard against the possibility of infection, is used solely to read memory cards containing vote results, accumulate and tabulate those results and produce reports, and (3) a separate computer dedicated solely to this purpose is used to reformat all memory devices before they are connected to the permanent system again. (This "air-gap" model was proposed by the Source Code Review Team that reviewed the Diebold Election Systems, Inc., GEMS 1.18.24 voting system. Further details concerning the model are provided in Section 6.10 of the Source Code Review of the Diebold Voting System, dated July 20, 2007, and available on the Secretary of State

website at http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf.)

3. Within 30 days of the date of this document, the vendor must submit to the Secretary of State for approval specifications for the hardware and operating system platform that must be used for all applicable components of the voting system. The vendor must identify the requirements for "hardening" the configuration of that platform, including, but not limited to:
   - BIOS configuration;
   - Identification of essential services that are required and non-essential services that must be disabled;
   - Identification of essential ports that are required and non-essential ports that must be disabled and, if feasible, removed or physically blocked;
   - Audit logging configuration;
   - Definition of user security roles and associated permissions to assure all users have only the minimum required permissions for their role;
   - Password policies, including password strength, expiration, and maximum attempts, along with all related user account control settings; and
   - All utilities and software applications, with specifications for their installation, configuration and use, that are necessary for operation of the voting system (e.g., security software, data compression utilities, Adobe Acrobat, etc.).

   The vendor must identify automated mechanisms for jurisdictions to confirm and document that their system has been configured to these standards, and that all updatable components are the approved version and level. The vendor must provide full instructions for the use of these mechanisms, including expected results.

4. Immediately after any repair or modification of any voting system component, the integrity of the firmware and/or software must be verified using the automated mechanisms described above, or all software must be reinstalled by the jurisdiction from a read-only version of the approved firmware and/or software supplied directly by the federal testing laboratory or Secretary of State before the equipment can be put back into service.

5. Jurisdictions are prohibited from installing any software applications or utilities on any component of the voting system that have not been identified by the vendor and approved by the Secretary of State.

6. Within 30 days of the date of this document, the vendor must develop and submit to the Secretary of State for approval, a plan and procedures for timely identification of required security updates (e.g., operating system security patches, security software updates, etc.), vendor testing of the updates, and secure distribution and application of vendor-approved security updates.

7. Within 45 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, uniform requirements and

use procedures for operating and maintaining the physical and logical security of the system, including, but not limited to:

- Physical security and access to the system and all components;
- Network security;
- Data security (including data backup requirements and procedures); and
- Separation of roles and responsibilities for jurisdiction personnel.

8. Network connections to any device not directly used and necessary for voting system functions are prohibited. Communication by or with any component of the voting system by wireless or modem transmission is prohibited at any time. No component of the voting system, or any device with network connectivity to the voting system, may be connected to the Internet, directly or indirectly, at any time.

9. Within 45 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, detailed uniform requirements and use procedures for programming, pre- and post-election logic and accuracy testing, transporting and operating voting equipment that will prevent or detect unauthorized access to or modification of any component of the voting system, including, but not limited to:

- Application of two-person rule;
- Chain of custody controls and signature-verified documentation;
- Requirements for secure interim storage of any system component; and
- Employment of mechanisms to detect unauthorized access to the equipment.

10. Where tamper-evident seals are required to detect unauthorized access to a system component, those seals must be serialized and the vendor must specify in each instance the type of the seal to be used and the exact placement of that seal using photographs.

11. Upon request, members of the public must be permitted to observe and inspect, without physical contact, the integrity of all externally visible security seals used to secure voting equipment in a time and manner that does not interfere with the conduct of the election or the privacy of any voter.

12. Where voting equipment is used to record and tabulate vote results in a polling place, upon close of the polls, the poll workers are required to print two copies of the accumulated vote results and audit log from each JBC or eScan. Each poll worker must sign every copy. One copy of the vote results and audit log from each device must be publicly posted outside the polling place. The second copy must be included with the official election material that is returned to the jurisdiction headquarters on election night.

13. No poll worker or other person may record the time at which or the order in which voters vote in a polling place.

14. Poll workers are not permitted to have access to any VBO audit records, nor may they participate in any audits or recounts involving VBO audit records.

15. Within 60 days of the date of this document, the vendor, working with jurisdiction users, must develop and submit to the Secretary of State for approval, specific detailed uniform requirements and use procedures for vote results auditing and reconciliation, review of audit logs and retention of election documentation to validate vote results and detect unauthorized manipulation of vote results, including, but not limited to:
    - Precinct level ballot accounting;
    - Identification of abnormal voting patterns on VBO audit trails;
    - Escalation of audit sampling when significant discrepancies exist between electronic and manual audit vote results; and
    - Reconciliation of discrepancies between electronic and manual audit vote results.

16. Any post-election auditing requirements imposed as a condition of this certification shall be paid for by the vendor. Jurisdiction users are required to conduct the audits and the vendor is required to reimburse the jurisdiction.

17. After consultation with jurisdiction users, the Secretary of State shall establish additional post-election manual count auditing requirements, including:
    - Increased manual count sample sizes for close races, based on an adjustable sample model, where the size of the initial random sample depends on a number of factors, including the apparent margin of victory, the number of precincts, the number of ballots cast in each precinct, and a desired confidence level that the winner of the election has been called correctly. In establishing sampling requirements for close races, the Secretary of State may impose a specific sampling threshold for a given vote differential or percentage of the margin of victory, taking into account the number of electors and the number and size of precincts in the race.
    - Escalation requirements for expanding the manual count to additional precincts when discrepancies are found.
    - Uniform procedures to increase transparency and effectiveness of post-election manual count audits.

18. Each polling place must be equipped with a method or log in a format specified by the Secretary of State after consultation with the jurisdiction users to record all problems and issues with the voting equipment in the polling place as reported by voters or observed by poll workers. Such records must include the following information for each event:
    - Date and time of occurrence;
    - Voter involved, if any;
    - Equipment involved;
    - Brief description of occurrence;
    - Actions taken to resolve issue, if any; and
    - Election official(s) who observed and/or recorded the event.

    All such event logs or reports must be made available to the public for inspection and review upon request. Prior to or concurrent with the certification of the election, the jurisdiction election official must submit a report to the Secretary of State of all reported problems experienced with the voting system and identifying the actions taken, if any, to resolve the issues.

19. Training of poll workers must include the following:
    - Secure storage of voting equipment while in the poll worker's possession;
    - Chain-of-custody procedures (including two person rule) required for voting equipment and polling place supplies;
    - Seal placement and procedures for verification of seal integrity;
    - Placement and observation of voting equipment;
    - Observation of activity that could indicate tampering or an attempt at tampering;
    - The Voter Bill of Rights set forth in section 2300 of the Elections Code;
    - The purpose served by the Voter Verified Paper Audit Trail (VVPAT), the importance of its use by voters, and how to handle problems such as paper jams;
    - A voter's right to vote on a paper ballot (in all DRE polling places) and how to handle requests for paper ballots;
    - The public right to inspect voting equipment and security seals, and how to handle requests for such inspections;
    - How to handle equipment failure or lack of sufficient paper ballots in a polling place and how to ensure continuity of the election in the event of such a failure; and
    - How to properly log all events and issues related to voting equipment in the polling place, including voter complaints of malfunctioning equipment.

20. All voters voting on paper ballots must be provided a privacy sleeve for their ballot and instructed on its use.

21. A warning must be posted in each voting booth stating that, pursuant to Elections Code sections 18564, 18565, 18566, 18567, 18568 and 18569, tampering with voting equipment or altering vote results constitutes a felony, punishable by imprisonment.

22. With respect to any piece of voting equipment for which the chain of custody has been compromised or for which the integrity of the tamper-evident seals has been compromised, the following actions must be taken:
    - The chief election official of the jurisdiction must be notified immediately;
    - The equipment must be removed from service immediately and replaced if possible;
    - Any votes cast on the device prior to its removal from service must be subject to a 100% manual audit as part of the official canvass;
    - Any memory card containing data from that device must be secured and retained for the full election retention period;
    - An image of all device software and firmware must be stored on write-only media and retained securely for the full election retention period; and
    - All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.

23. If a voting device experiences a fatal error from which it cannot recover gracefully (i.e., the error is not handled through the device's internal error handling procedures with or without user input), such that the device must be rebooted or the device reboots itself to restore operation, the following actions must be taken:
    - The chief election official of the jurisdiction must be notified immediately;

- The equipment must be removed from service immediately and replaced as soon as possible;
- Any votes cast on the device prior to its removal from service must be subject to a 100% manual audit over and above the normal manual audit conducted during the official canvass;
- Any memory card containing data from that device must be secured and retained for the full election retention period;
- An image of all device software and firmware must be stored on write-only media and retained securely for the full election retention period;
- The vendor shall provide an analysis of the cause of the failure;
- Upon request by the Secretary of State, the vendor shall retain the device for a reasonable period of time to permit forensic analysis; and
- All device software and firmware must be reinstalled from a read-only version of the approved firmware and software supplied directly by the federal testing laboratory or the Secretary of State before the equipment is placed back into service.

24. The Secretary of State will review and finalize all plans, requirements and procedures submitted pursuant to the foregoing requirements above within thirty days of receipt. Upon approval, all such plans, requirements and procedures will automatically be incorporated into the official use procedures for the voting system, and will become binding upon all users of the system.

25. No substitution or modification of the voting system shall be made with respect to any component of the voting system, including the Use Procedures, until the Secretary of State has been notified in writing and has determined that the proposed change or modification does not impair the accuracy and efficiency of the voting system sufficient to require a re-examination and approval.

26. The Vendor developed utilities, Fusion, In-Fusion, Bravo and Trans, are specifically excluded from this certification.

27. The Secretary of State reserves the right, with reasonable notice to vendor and to the counties using the voting system, to modify the Use Procedures used with the voting system and to impose additional requirements with respect to the use of the system if the Secretary of State determines that such modifications or additions are necessary to enhance the accuracy, reliability or security of any of the voting system. Such modifications or additions shall be deemed to be incorporated herein as if set forth in full.

28. Any county using this voting system shall, prior to such use in each election, file with the California Secretary of State a copy of its Election Observer Panel plan.

29. The vendor agrees in writing to provide, and shall provide, to the Secretary of State, or to the Secretary of State's designee, within 30 days of the Secretary of State's demand for such, a working version of the voting system, including all hardware, firmware and software of the voting system, as well as the source code for any software or firmware contained in the voting system, including any commercial off the shelf software or firmware that is available and disclosable by the vendor, provided that the Secretary of

State first commits to the vendor in writing to maintain the confidentiality of the contents of such voting system or source code so as to protect the proprietary interests of the vendor in such voting system or source code. The terms of the commitment to maintain confidentiality shall be determined solely by the Secretary of State, after consultation with the vendor. The voting system shall not be installed in any California jurisdiction until the vendor has signed such an agreement. Any reasonable costs associated with the review of the source code for any software or firmware contained in the voting system shall be borne by the vendor.

30. The Secretary of State reserves the right to monitor activities before, during and after the election at any precinct or registrar of voters' office, and may, at his or her discretion, conduct a random parallel monitoring test of voting equipment.

31. By order of the Secretary of State, voting systems certified for use in California shall comply with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. Further, voting systems shall also comply with all state and federal voting system guidelines, standards, regulations and requirements that derive authority from or are promulgated pursuant to and in furtherance of the California Elections Code and the Help America Vote Act of 2002 or other applicable state or federal law when appropriate.

32. Voting system manufacturers or their agents shall assume full responsibility for any representation they make that a voting system complies with all applicable state and federal requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002. In the event such representation is determined to be false or misleading, voting system manufacturers or their agents shall be responsible for the cost of any upgrade, retrofit or replacement of any voting system or its component parts found to be necessary for certification or otherwise not in compliance.

33. Any voting system purchased with funds allocated by the Secretary of State's office shall meet all applicable state and federal standards, regulations and requirements, including, but not limited to, those voting system requirements as set forth in the California Elections Code and the Help America Vote Act of 2002 and those requirements incorporated by reference in the Help America Vote Act of 2002.

34. The vendor must establish a California County User Group and hold at least one annual meeting where all California users and Secretary of State staff are invited to attend and review the system and ensure voter accessibility.

35. In addition to depositing the source code in an approved escrow facility, the vendor must deposit with the Secretary of State a copy of the system source code, binary executables and tools and documentation, to allow the complete and successful compilation and installation of a system in its production/operational environment with confirmation by a

verification test by qualified personnel using only this content. The Secretary of State reserves the right to perform a full independent review of the source code at any time.

36. The vendor must provide printing specifications for paper ballots to the Secretary of State. The Secretary of State will certify printers to print ballots for this system based upon their demonstrated ability to do so. The vendor may not require exclusivity in ballot printing and must cooperate fully in certification testing of ballots produced by other ballot printers.

IN WITNESS WHEREOF, I hereunto set my hand and affix the Great Seal of the State of California, this 3rd day of August, 2007.

DEBRA BOWEN
Secretary of State